

Best Available Copy

# SECURE SYSTEM FOR ACTIVATING PERSONAL COMPUTER SOFTWARE AT REMOTE LOCATIONS

Patent number: JP6501120T

Publication date: 1994-01-27

Inventor:

Applicant:

Classification:

- international: G06F13/00; G06F15/00; H04L9/00; H04L9/00;  
H04L9/10; H04L9/12

- european: G06F1/00N7R2; G06F9/445; G06F9/445N;  
G06F21/00N7P5M

Application number: JP19910501845T 19911106

Priority number(s): US19900610037 19901107; US19910682456 19910409

Also published as:

WO9209160 (A1)  
EP0556305 (A1)  
US5222134 (A1)  
EP0556305 (A4)  
EP0556305 (B1)

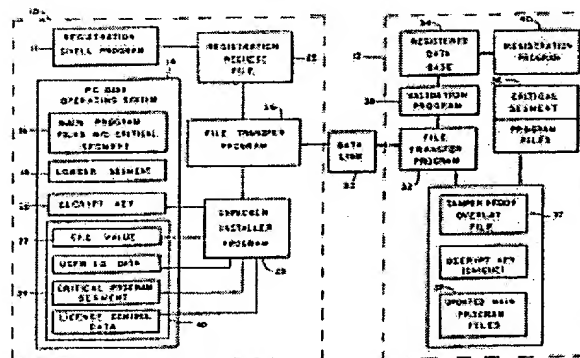
more >>

Report a data error here

Abstract not available for JP6501120T

Abstract of corresponding document: **US5222134**

A process and system for activating various programs are provided in a personal computer. The computer is initially provided with a registration shell. A data link is established between the personal computer and a registration computer. By providing the registration computer with various information, a potential licensee can register to utilize the program. Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer and transferred to the personal computer. The tamperproof overlay includes critical portions of the main program, without which the main program would not operate and also contains licensee identification and license control data.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平6-501120

第6部門第3区分

(43) 公表日 平成6年(1994)2月3日

(51) Int.Cl.	識別記号	序内整理番号	F I
G 0 6 F 13/00	3 5 1 H	7368-5B	
15/00	3 3 0 A	7459-5L	
H 0 4 L 9/00			
9/10			
	7117-5K	H 0 4 L 9/00	Z
	審査請求 有	予備審査請求 有	(全 8 頁) 最終頁に続く

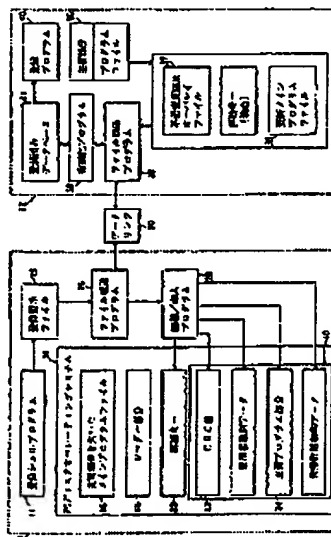
(21) 出願番号 特願平4-501845  
 (86) (22) 出願日 平成3年(1991)11月6日  
 (85) 翻訳文提出日 平成5年(1993)5月7日  
 (86) 国際出願番号 P C T / U S 9 1 / 0 8 0 6 9  
 (87) 国際公開番号 W O 9 2 / 0 9 1 6 0  
 (87) 国際公開日 平成4年(1992)5月29日  
 (31) 優先権主張番号 6 1 0 , 0 3 7  
 (32) 優先日 1990年11月7日  
 (33) 優先権主張国 米国 (U S)  
 (31) 優先権主張番号 6 8 2 , 4 5 6  
 (32) 優先日 1991年4月9日  
 (33) 優先権主張国 米国 (U S)

(71) 出願人 タウ システム コーポレーション  
 アメリカ合衆国 バージニア州 フォルス  
 チャーデ, リースバーグ バイク,  
 7115, スーツ327  
 (72) 発明者 ワイト, デービッド, ビー  
 アメリカ合衆国 バージニア州 22032,  
 フェアファックス ギルバートソン ロー  
 ド, 4220  
 (72) 発明者 リッデル, ホレイス, ジー  
 アメリカ合衆国 バージニア州 22021,  
 チャンチリイ, バレイ カウントリ ドラ  
 イブ, 13811  
 (74) 代理人 井端士 倉持 裕 (外1名)  
 最終頁に続く

(54) 【発明の名称】 パーソナルコンピュータのソフトウェアを遠隔位置で起動するための安全システム

## (57) 【要約】

様々なプログラムを起動するための過程とシステムがパーソナルコンピュータ(10)に提供されている。パーソナルコンピュータ(10)には、登録シェルスプログラム(11)が当初備わっている。データリンク(80)がパーソナルコンピュータ(10)と登録用コンピュータ(12)の間に確立される。登録用コンピュータ(12)に様々な情報を与えることにより、見込み被許諾者はメインプログラム(16)の使用を登録することができる。ひとたび登録過程が完了すると、不正変更防止オーバーレイプログラムが登録用コンピュータ(12)において作成され、パーソナルコンピュータ(10)に転送される。不正変更防止オーバーレイには、メインプログラム(16)の主要部分がふくまれ、これを欠くとメインプログラム(16)は動作せず、また不正変更防止オーバーレイには使用許諾識別データと使用許諾制御データも含まれている。



## 【請求の範囲】

1. プログラムファイルを起動する方法であって、  
 該装置を有する基端コンピュータに対して、ロードセグメントと登録シェル部分を含むプログラムファイルを提供し、上記プログラムファイルは主要部分を欠いて、上記プログラムファイルを正しく実行することを防止する工程、  
 使用登録情報を上記登録シェル部分に入力する工程、  
 上記使用登録情報を、上記登録シェルから登録用コンピュータ内にあらかじめインストールした登録プログラムに転送し、上記登録プログラムは使用登録データと上記登録部分を結合して独自のオーバーレイファイルを作成する工程、  
 上記独自のオーバーレイファイルを上記登録プログラムから上記登録シェルに転送する工程、上記オーバーレイファイルには上記プログラムファイルには記載されていない主要部分が含まれ、そして  
 上記オーバーレイファイルを上記メインプログラムファイルに導入する工程を有し、上記オーバーレイファイルに入っている使用登録情報が導入されたときだけ上記プログラムファイルの動作が可能であることを特徴とする特記のプログラムファイル起動方法。
2. 上記オーバーレイファイルを上記登録用コンピュータから上記基端コンピュータに転送する前に、上記使用登録情報を利用可能にする工程を有する請求の範囲第1項に記載の方法。
3. 不正変更防止のオーバーレイファイルを作成する工程を有する請求の範囲第1項に記載の方法。
4. 上記不正変更防止オーバーレイファイルが上記オーバーレイファイルを暗号化することにより作成され、巡回冗長検査値が上記

主要プログラム部分が欠けているプログラムファイルが当該偶々について、このプログラムファイルが動作することを防止し、上記オーバーレイロード部分は本物のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記基端コンピュータには登録シェルプログラムが備えられ、上記登録シェルプログラムは使用者が様々な使用登録情報を入力することと可能にするような少なくとも一台の基端コンピュータと、

登録プログラムと、上記使用登録情報を登録し処理するための手段と、上記プログラムファイルに欠けている上記主要プログラム部分と使用登録情報の全部あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記基端コンピュータに転送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記基端コンピュータに転送することで、上記オーバーレイファイルに入っている使用登録情報が現在導入されているときだけ上記プログラムファイルの動作が可能になることを特徴とする上記プログラムファイル起動システム。

13. 上記基端コンピュータと上記登録用コンピュータとの間を結合する電子データリンクと、上記登録用コンピュータと上記基端コンピュータの両方に備えられているファイル転送装置とを含むことを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

14. 上記登録用コンピュータが、すべての登録済み使用者が含まれている中央データベースと上記使用登録情報を有格化するための手段とを備えていることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

## 特表平6-501120 (2)

暗号化オーバーレイファイル内にあるとともに、暗号キーを上記オーバーレイファイルに格納する請求の範囲第8項に記載の方法。

6. 上記オーバーレイが実行のためにロードされるたびに巡回冗長検査値が計算され、上記不正変更防止オーバーレイファイル内に転送された巡回冗長検査値と比較され、上記オーバーレイファイルが暗号化後変更されているかどうかを判断することを特徴とする請求の範囲第1項に記載の方法。

6. 上記使用登録情報と上記オーバーレイファイルとが、電子データリンクを介して上記登録シェルと上記登録プログラムとの間を転送されることを特徴とする請求の範囲第1項に記載の方法。

7. 上記登録シェルプログラムが、上記のインストールした登録用コンピュータを備えた基端コンピュータから離れた、第一のコンピュータ内に格納されていることを特徴とする請求の範囲第1項に記載の方法。

8. 上記利用可能工程によって上記使用登録情報が正式の登録シェルを確保することを特徴とする請求の範囲第8項に記載の方法。

9. 上記使用登録と上記オーバーレイファイルが、一台のコンピュータに入力され備えられることを特徴とする請求の範囲第1項に記載の方法。

10. プログラムファイルを削除されたもしくは削除されない両方の場合に於いて、

オーバーレイロード部分が含まれている少なくとも一つの

13. オーバーレイファイルを作成するための上記手段が、巡回冗長検査値を備える不正変更防止オーバーレイファイルを作成するための暗号化装置と暗号キーを備えており、上記暗号キーは上記オーバーレイファイルと共に上記登録用コンピュータに転送されることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

14. 上記基端コンピュータが、上記オーバーレイファイルを解放し、上記オーバーレイファイルが実行のためにロードされるたびに巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータによって上記オーバーレイファイルと共に転送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第12項に記載のプログラムファイル起動システム。

15. 上記主要部分がエグゼクティブ制御部分であり、そして上記使用登録情報が使用許諾契約情報であることを特徴とする請求の範囲第1項に記載の方法。

16. 上記主要プログラム部分がエグゼクティブ制御プログラムであり、そして上記使用登録情報が使用許諾契約情報であることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

17. 上記主要エグゼクティブ制御プログラム部分がプログラムファイル全体を有することを特徴とする請求の範囲第16項に記載のプログラムファイル起動システム。

18. プログラムファイルの使用を制御する方法において、  
 該装置を有するコンピュータに対してロード部分と登録シェル部分を含むプログラムファイルを提供し、上記プログラムフ

ファイルは第一レベルの制御機能を有するエグゼクティブ制御プログラムを有しており、

情報を上記登録シェル部分に入力し、

上記使用許諾契約情報を上記登録シェルから独立登録プログラムに伝送し、上記登録プログラムは使用許諾契約データを第二レベルの制御機能を有するエグゼクティブ制御プログラムに併合して独自のオーバーレイファイルを作成し、

上記独自のオーバーレイファイルを上記登録プログラムから上記登録シェルに伝送し、上記オーバーレイファイルには上記第二レベルのエグゼクティブ制御プログラムが含まれており、そして

上記独自のオーバーレイファイルを上記主要プログラムファイルに導入し、上記プログラムファイルの第二レベルの機能の動作が上記オーバーレイファイル内の使用許諾契約情報が要求導入されているとみられることと特徴とする上記のプログラムファイル使用の制御方法。

19. 上記オーバーレイファイルを上記登録用コンピュータから上記登録コンピュータに伝送する以前に、上記使用許諾契約情報を有効化する工程を有する請求の範囲第18項に記載の方法。

20. 不正変更防止になっているオーバーレイファイルを作成する工程を有する請求の範囲第18項に記載の方法。

21. 上記不正変更防止オーバーレイファイルが上記不正変更防止オーバーレイファイルを暗号化キーで暗号化することにより作成され、巡回冗長検査値を上記暗号化不正変更防止オーバーレイファイル内に提供するとともに暗号キーを上記不正変更防止オーバーレイファイルに提供し、上記暗号化および暗号キーは上記オーバーレイファイルの独自の内容によって独自に決定されることを特徴とする請求の範囲第20項に記載の方法。

上記登録シェルプログラムは使用者が様々な使用許諾契約情報を入力することを可能にするよう少なくとも一回の遠隔コンピュータと、

登録プログラムと、上記使用許諾契約情報を受信し処理するための手段と、第二レベルの機能を有するプログラムモジュールと使用許諾契約情報の全部あるいは一部を含む独自のオーバーレイファイルを生成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記遠隔コンピュータに伝送することで、上記オーバーレイファイルに入っている使用許諾契約情報が伝達されているとみられ、上記プログラムファイルの第二レベルの機能動作が可能なることを特徴とする上記システム。

22. 上記遠隔コンピュータと上記登録用コンピュータとの間に電子データリンクを有し、ファイル転送過程が上記登録用コンピュータと上記遠隔コンピュータの両方に備えられていることを特徴とする請求の範囲第17項に記載のシステム。

23. 上記登録用コンピュータが、すべての登録済み使用権が含まれる中央データベースと上記使用許諾契約情報を有効化する手段とを備えていることを特徴とする請求の範囲第22項に記載のシステム。

24. オーバーレイファイルを生成するための上記手段が、巡回冗長検査値が記憶されている不正変更防止オーバーレイファイルを作成するための暗号化キーと暗号キーとを備えており、上記暗号キーは上記オーバーレイファイルと共に上記遠隔コンピュータに伝送され、上記暗号化および暗号キーはファイルの内容によって独自に決定されることを特徴とする請求の範囲第23項に記載のシステム。

### 30 表平6-501120 (9)

22. 新しい巡回冗長検査値が、上記オーバーレイが実行のためにロードされるたびに計算されて、上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較され、上記オーバーレイファイルが作成以降変更されているかどうかを判断することを特徴とする請求の範囲第21項に記載の方法。

23. 上記使用許諾契約情報と上記オーバーレイファイルが、上記登録シェルと上記登録プログラムとの間に電子データリンクを介して伝送されることを特徴とする請求の範囲第18項に記載の方法。

24. 上記登録シェルプログラムが、上記独立登録プログラムを備えた第二のコンピュータから離れている第一のコンピュータに備えられていることを特徴とする請求の範囲第18項に記載の方法。

25. 上記有効化により上記使用許諾契約情報が正式に登録シェルを介して確保することを特徴とする請求の範囲第19項に記載の方法。

26. 上記使用許諾契約情報と上記オーバーレイファイルが一組のコンピュータに導入され、備えられていることを特徴とする請求の範囲第18項に記載の方法。

27. 破壊されたあるいは削除されない期間、プログラムファイルをアップグレートするシステムにおいて、

第二レベルの機能を有するプログラムを含むオーバーレイローダー部分を含むプログラムファイルが記憶されていて、上記オーバーレイローダー部分は単独のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記遠隔コンピュータには登録シェルプログラムが備えられ、

システム。

21. 上記遠隔コンピュータが、上記オーバーレイファイルを解読し、上記オーバーレイファイルが実行のためのロードされるたびに所しい巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータにより上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第20項に記載のシステム。

## 【明 細 書】

パーソナルコンピュータのソフトウェアを遠隔位置で起動するための資金システム

## 発明の背景

一般的に、パーソナルコンピュータあるいはそれに類似した装置の使用者の大部分は、それら装置で実行するソフトウェアを様々な小売店からあるいは直接販売を通じて入手する。いずれの場合も、ソフトウェア製品はいわゆる「紙箱包装」材で包装されており、その紙箱包装材を開いた時点でそのソフトウェア製品に対する使用許可契約が成立して、その製品の使用許諾者も使用許諾者/購入者による使用可能期間あるいは使用から保護するようにになっている。この方法による商行為は、許諾者と被許諾者の双方にとって満足すべきものではないことが分かっている。たとえば、被許諾者にとっては、ソフトウェアプログラムを動作させてみてからそれが被許諾者が必要としているものかどうかを判断する機会が与えられない。さらに、許諾者の側からみると、この方法では被許諾者の識別ができないうえ、許諾者によるプログラム使用の制御あるいは監視を行なうことができない。

ソフトウェアプログラム保護方法は、Thomsonの米国特許第4,446,519号に開示されており、プログラミングされた「はい/いいえ」で答える装置がプログラムに組み込まれており、そのソフトウェアが使用許可されるコンピュータに設置されているハードウェアあるいはファームウェア保護装置の存在を判断するようになっている。この装置の装置は、プログラムが物理的な複製をなしでは使用できないようにすることであり、これはソフトウェアよりも複製することがはるかに困難である。しかし、このような装置は、正しい符号化応答が見られ、そしてそれをわずかに変更してプログラムに書き込まれてしまえば、簡単に打ち破られてしまう。ひとたび打ち破られると、無制限の遠征コピーが作成され配布される可能性がある。

照する方法とシステムに関する。動作可能プログラムは、購入者/被許諾者と販売者/許諾者との間の特定の契約において入手可能になる。販売者と購入者との関係は、本発明の目的に照しては、許諾者/被許諾者間の関係である必要はないが、以下では販売者と被許諾者、購入者も被許諾者もしくは使用者と呼ぶ。ひとたび被許諾者が特定の契約条件に同意すると、被許諾者識別データが登録用コンピュータに与えられる。登録用コンピュータはその契約を記録し、使用許可されたプログラムの可動部分を渡す。これらの部分は不正変更防止が施されていると同時に、識別された被許諾者にとって独自のものとなっている。この情報の交換に基つき、可動コンピュータプログラムが登録用被許諾者のコンピュータに不正変更防止ファイルに収納されて配布される。同時に、このファイルには販売者独自の情報が含まれている。本発明の実施例としては様々なものが考えられるが、いずれの実施例も被許諾者を識別する独自のデータと保護されているソフトウェアプログラムに関する情報とが含まれている符号化パッケージの構造を伴っている。したがって、被許諾者は複製ではなく、そして保護されたソフトウェアは使用許諾契約に違反できる情報で付帯化される。さらに、使用許可制御データを符号化パッケージに含めることにより、様々な複製を許して使用許可契約の条件を遵守させることができる。

一般的に、様々な実施例は、ソフトウェアのデモンストレーション版を有する可能性のあるマーケティングシミュレーションプログラムの最初の配布が伴う。このシミュレーションプログラムは、見本表示と直訳記述だけを有しているか、あるいは完全なプログラムの動作不能版を有している。しかし、大部分の実施例は、登録プログラムと、ローダーセグメントと呼ばれる特定のプログラムモジュールを含むような構成になっている。

マーケティングシミュレーションは適切な方法で自由に配布されるであろう。マーケティングシミュレーションプログラムのデモンストレーション

## 特表平6-501120 (4)

Willieの米国特許第4,740,830号は、中央(遠隔)コンピュータを使用して、正しい符号の入手を試みる意図のプログラムがアクティブでないマスターリストあるいはアルゴリズムから得られたコア解除コードあるいは有効化コードを提供することを開示している。しかし、この方法は、伝送中のコードを侵害することにより、あるいは保護の周回をプログラミングすることにより、もしくはデバッガープログラムによりプログラムを分析してプログラムの実行を可能にするコードの存在を見つ出すことにより、簡単に見破られてしまう。ひとたびこの保護が打ち破られると、動作可能なプログラムの無制限のコピーが作成され配布される可能性がある。

さらに、Schmidtの米国特許第4,649,510号に開示されている方法では、最も価値のあるアルゴリズムを新設化し、無効化されたプログラムを処理装置内で実行すると同時に、回復アルゴリズムを別の物理的に分離し保護された処理装置で実行することにより回復し、前記結果をその処理装置の増設装置によって獲得するようになっている。このような方法は、回復アルゴリズムの物理的保護に依存しており、この物理的保護が侵害された場合、悪意のプログラムによって簡単に打ち破られる可能性がある。したがって、そのような方法は、回復記憶媒体の物理的保護が維持できない大量市場においては、実用的ではない。

そのため、ソフトウェアを登録可能使用から保護しつつソフトウェアを大量市場に配布するための経済的な方法が求められる。さらに、見込み購入者/被許諾者がソフトウェア製品を購入前に試してみることができよう方法とシステムも必要である。また、ソフトウェア製品の改良および更新部分と登録使用者に配布するための方法も必要である。

## 発明の簡単な説明

本発明は、パーソナルコンピュータのソフトウェアプログラムあるいは他の種類のプログラムを、使用許可を管理する方法で配

版を有している場合、ニグゼクティブ知照ループが保護されたプログラムの販売版になる。マーケティングシミュレーションは見込み使用者に登録を促す。マーケティングシミュレーション内の登録プログラムは、登録データと登録データベースコンピュータに送られる。符号化ファイル内で結合された実行時使用可能なデータと動作可能版のプログラムとを有する独自の符号化パッケージが組み立てられる。独自の符号化パッケージが、符号化ファイルおよび保護されていないプログラムファイルと共に使用者のコンピュータに渡される。これらはマーケティングシミュレーションを最大化させる。解読キー、符号化ファイル、そして保護されていないファイルの削除と同時に、マーケティングシミュレーションはこれらのデータを使用者のコンピュータに導入する。

したがって、使用者がプログラムを実行する毎に、ローダーセグメントが提供された解読キーを使用して、符号化ファイルを保護されていないファイルに対するオーバーレイとしてロードして解読する。このプログラムは保護されていないソフトウェアプログラムの設計にしたがって実行され、独自の使用許諾データもプログラム実行中にロードされる。プログラムが実行されていないときは、保護されているプログラムはその符号化形態に留まって、保護されていないプログラムファイルと共にコンピュータの大容量記憶装置に格納されている。保護されているプログラムは実行のためにロードされたときだけ解読され、正しい符号化キーにアクセスしなければ実行されない。

## 図面の簡単な説明

- 図1は本発明による登録過程を示す流れ図である。  
図2は本発明によるプログラム実行過程を示す流れ図である。  
図3は、本発明の知見による代表的なパーソナルコンピュータと登録用コンピュータの構成図である。  
図4は、本発明の知見による代表的なパーソナルコンピュータと登録用コンピュータに代る実施例を示す構成図である。

### 発明の詳細な説明

本発明の目的は、許諾者がそのプログラムの費用対効果に関する調査を従来使用されている方法よりはるかに効率的な方法で維持することを可能にすることである。さらに、本発明の第二の目的は、被許諾者あるいは使用者が特定のプログラムの購入あるいは使用許諾を得る前に試用することも可能にすることである。さらに、本発明の更なる目的は、特定のプログラムの使用許諾保護されたアップグレード経路を被許諾者に提供することも可能にすることである。したがって、本発明の目的は包括的なものと見られ、そしてどのようなソフトウェアプログラムも本方法によって配布できるものと見なされている。

一実施例において、動作可能なエグゼクティブ制御ループを除いて完全な複製プログラムが、パーソナルコンピュータあるいは他の装置において、磁気ディスク、フロッピーディスク、ハードウェアあるいは他の手段で最初に提供される。さらに、この複製プログラムには登録シリアルプログラムも含まれる。ただし、小さいプログラムもしくは低価のあるプログラムの場合、プログラム自体は存在せず、シリアルだけが提供される。エグゼクティブ制御ループが除外されているため、このプログラムは正しい複製過程を実現しなければ動作しない。図1および図2に示されているように、この登録過程は、パーソナルコンピュータ(PC) 10内部の登録シリアルプログラム11と登録用コンピュータ12内部に提供されている登録プログラム40とを使用して開始される。登録システムプログラムが登録用コンピュータ12内部に提供され、電子データリンク30を介して登録シリアルプログラムがアクセスできる。この電子データリンクは、ローカルエリアネットワークでもよく、電話モデムリンクでもよく、あるいはその他のいかなる形態であってもよい。ただし、第二の実施例においては、登録シリアルおよび登録システムプログラムは同一の媒体上に存在してもよいが、その媒体は製品応用プログラムとは別でなければならない。この場

### 特表平6-501120(5)

合、登録シリアルおよび登録システムプログラムが入っている対応可能な媒体は、許諾された導入プログラムによって使用可能なパーソナルコンピュータ10へ個人的に移植され、電子データリンクは必要ではない。

登録シリアルプログラムは、使用者がPCオペレーティングシステム14のメインプログラムファイル内に提供されている製品応用プログラムの実行を最初に実行すると実行される。登録シリアルは、製品応用プログラムに関する記述情報を提供しそれをPC表示装置に表示すると同時に、見込み被許諾者を促して候補者として登録する。使用許諾は、特定の追加条件における特定の被許諾者に対して提供され、その期間は様々な長さもしくは一時的でよく、そのための費用は被許諾者に対して課せられない。ただし、登録シリアルは、不正変更防止スーパーレイファイルが存在しないかどうか、メインプログラムを実行しない。登録シリアルプログラム11は、被許諾者のPCに実行されるとデータ入力形式を提供し、被許諾者に対して、請求書送付先、口座番号、使用許諾条件などの識別情報の提供を要求する。この情報は、被許諾者が再登録する登録要求ファイル25に入力される。そして、登録シリアルプログラムは、被許諾者が特定のキーを押して登録を開始するのを待つ。このキーが押されると、登録ファイルが同じ。そして登録シリアルファイル転送プログラム26が登録システムファイル転送プログラムとのデータリンクを確立する。登録用コンピュータ内の登録プログラム40は、データリンクが正常な登録シリアルで確立されていることを確認する検索保護チェックを実行する増強手段42によって保護される。つぎに、登録シリアルは登録要求ファイル25と、そのファイルを受信する登録システムに転送し、必要なインターチェンジと、結合されたファイル転送プログラム26および32間のハンドシェイク動作を実行する。完全な登録要求ファイルが中央登録用コンピュータで受信されると、登録要求が登録済み使用者34のデータベースに対して確認される。確認には、その要求に答えるべきかど

うかを判断する様々なチェックが含まれる。たとえば、一時的使用許諾に対する要求が特定の被許諾者から再度送られてきた場合、その被許諾者には使用許可が与えられず、そしてそのプログラムのエグゼクティブ制御ループは過期されない。そのような状態が発生した場合、適切なメッセージが登録シリアルに転送され、見込み被許諾者に対して表示される。しかし、要求が確認されると、登録済み使用者データベースへの記録が修正されるが、この過程全体が完了するまで、そのデータベースには入力されない。

登録用コンピュータ12の内部では、つぎに使用許諾データが使用されて、使用許諾データとエグゼクティブ制御ループプログラム命令36とを結合することにより作成された独自の不正変更防止スーパーレイファイルが生成される。生成されたデータとプログラムファイルとを照合し、不正変更防止スーパーレイファイル37内に含まれる巡回冗長検査(CRC)値が計算される。一式の独自の暗号化キーと解読キーが作成され、不正変更防止スーパーレイファイルの内容全体が暗号化キーを使用して暗号化される。この暗号化キーに基づき、不正変更防止スーパーレイファイルと共に提供される暗号化キーが提供される。暗号化アルゴリズムは、巡回暗号化システムのように、暗号化と解読にそれぞれ異なるキーを使用する状態であればなんでもよい。登録システムが、不正変更防止スーパーレイファイルと解読キーを、パーソナルコンピュータ登録シリアルに転送される1個の応答ファイル38に組み込む。また、更新されたメインプログラムファイルもこの応答ファイルに組み込まれ、ファイル転送プログラムとすでに確立されているデータリンクとを介してPCの登録システムに転送される。

出所ファイル一式の受信と同時に、登録シリアルプログラム内の開閉-導入プログラム11が応答ファイルを開き、エグゼクティブ制御ループセグメント16、CRC値22ならびに解読キー32および、含まれている場合は、更新メインプログラムファイルを含む不正変更防止スーパーレイファイル40を読み取る。これで登録過程が

完了したので、電子データリンクを切断する。登録データベースレコードが入力され、そして被許諾者の要求に対する請求が、中央登録用コンピュータ12における別のプログラムによって実行される。

登録が終了すると、被許諾者のパーソナルコンピュータに導入された製品項製品応用プログラムを起動して、不正変更防止スーパーレイファイルと解読キーを使用して製品応用プログラムを実行するときに実行する製品応用プログラム一式をロードするためのプロセスが開始される。

このプログラム実行過程を図1に示す。図示されているように、パーソナルコンピュータの使用者が製品応用プログラムの実行をオペレーティングシステムに命令すると、オペレーティングシステムはメインプログラムとローダーセグメントをロードする。ローダーセグメントは他のすべてのプログラム命令に先立って実行される。つぎに、ローダーセグメントは製品応用プログラムの起動を実行し、不正変更防止スーパーレイの存在をチェックする。不正変更防止スーパーレイが導入されていないければ、ローダーセグメントは終了してオペレーティングシステムに戻る。メインプログラムファイルの実行が事前に防止される。不正変更防止スーパーレイが導入されていれば、ローダーセグメントは解読キーを見つけて不正変更防止スーパーレイの解読とロードを行ない、メインプログラムファイルに対して存在しないエグゼクティブ制御ループプログラム命令ならびに独自の識別および使用許諾制御データを照合させる。解読およびロード過程において巡回冗長検査が実行され、それが完了すると、不正変更防止スーパーレイが登録用コンピュータからパーソナルコンピュータに転送されたときに作成された不正変更防止スーパーレイに記憶された巡回冗長検査値と比較される。巡回冗長検査値が失敗に終わると、そのスーパーレイは知らぬ方法によって変更が加えられたものとみなされ、したがって無効とされる。この時点で、ローダーセグ

## 特表平6-501120 (8)

ントはそのオーバーレイを取り外し、終了してオペレーティングシステムに戻る。したがって、不正変更防止オーバーレイが含まれていない場合と同様に、メインプログラムファイルの実行は、不正変更防止オーバーレイのどの部分が変更されていても、事前に防止される。返戻元長検査の結果、オーバーレイが変更されていないことが確認されると、ローダーセグメントはオーバーレイを含むメインプログラムファイルの実行を開始し、そして製品応用プログラムが最後まで実行される。

不正変更防止オーバーレイを動作可能状態の製品応用プログラムに含めることを要求することにより、被読者識別と使用許諾制御データがそれ以降動作可能プログラムに常に含まれることになる。このようにして、被読者は不正使用を防止するとともに監視することができる。

図1および図2を参照しながら説明したように、本発明によると、登録過程によって、メインプログラムファイルのニグゼクティブ制御ルーブセグメントと使用許諾制御データとを含む不正変更防止オーバーレイファイルが生成される。登録過程が完了すると、この不正変更防止オーバーレイは登録用コンピュータからパーソナルコンピュータに転送される。この不正変更防止オーバーレイは、起動時に不正使用を防止するキー装置である。なぜなら、エグゼクティブ制御ルーブプログラム命令は、均等なしに独自の使用許諾制御データと使用許諾制御データから分離することによって、被読者識別と使用許諾制御データも均等なしには変更できないからである。

この不正変更防止オーバーレイファイルは、オーバーレイファイルが印付されるときに最初に返戻元長検査値をオーバーレイファイルに記憶させると不正変更防止になるとみなされる。返戻元長検査値は、プログラム命令と使用許諾データを含有オーバーレイファイルの内容全体に対して計算される。被読者データは製品であるので、各々のCRCは秘密なものになる。記憶されてい

るCRC値が、オーバーレイがロードされるたびローダーセグメントによって計算された返戻元長検査値と比較される。これらの返戻元長検査値が一致しなければ、ローダーセグメントは終了してオペレーティングシステムに戻る。したがって、オーバーレイファイルの内容になんらかの変更が加えられていれば、記憶されている返戻元長検査値に一致する変更が行われないかぎり、そのオーバーレイファイルは無効になる。つぎに、不正変更防止オーバーレイの内容全体が、返戻元長検査値の位置が不明になるような方法で暗号化されるので、この値の存在をきつめてそれを変更することが困難になる。

また、暗号化により、不正変更防止オーバーレイに含まれる特定のプログラム命令とらびに独自の被読者識別および使用許諾制御データがはつきりしなくなる。暗号化は、公開鍵暗号化システムのように暗号化と解読に別々のキーを使用する状況によって達成される。暗号化ならびに独自の暗号化キーおよび解読キー発生のためのアルゴリズムは登録システム内に登録し、したがって被読者にはアクセスが不可能である。解読キーは、登録システムに登録プログラムシリアルを通じて被読者のコンピュータに転送される。オーバーレイファイルを解読するためのアルゴリズムはローダーセグメント内にあるので、解読キーと解読アルゴリズムを使用してオーバーレイファイルを解読しその内容を検証することは、困難ではあるが可能である。しかし、内容を変更して、新しい変更されたオーバーレイファイルを暗号化する試みは、暗号化キーに対するアクセスができないために阻止される。私的暗号化キーで暗号化されたオーバーレイファイルだけでは公開鍵解読キーで解読できず、私的キーは公開キーから容易には得られないというのが、公開鍵暗号化システムの特徴である。

不正変更防止オーバーレイファイルは、プログラム命令のエグゼクティブ制御ルーブセグメントと、使用許諾の方法と制御に適切な独自の被読者識別データとを有している。このデータには、

使用許諾の期間、コンピュータの製造番号、コンピュータのモデルの電圧番号、そしてその他の情報が含まれる。

ローダーセグメント18は登録目的のサブプログラムであり、これは、ローダープログラムが取り除かれたり返戻された場合、メインプログラムファイルを動作不能にする状況によって製品応用プログラムのメインプログラムファイルに結合される。この結合状況は、特定のプログラム命令と製品応用プログラムのメインプログラムファイル内部に内蔵するプロセスである。これらの内蔵された命令は、使用率によっては特定の記憶位置にある特定の値を検査する。ローダープログラムセグメントを実行すると、特定の値がメインプログラムファイルの動作を可能にするのに必要な特定の記憶アドレス位置に記憶される。ローダープログラムセグメントは、その他の後述の図にこの動作を実行する。したがって、ローダーセグメントを取り外したり返戻したりすると、メインプログラムファイルには特定の位置における特定の値が含まれないことになり、そのため動作不能になる。

図の実施例において、登録シェルは、製品応用プログラムの動作可能なデモンストレーション版を含んでいる可能性があるマーケティングパッケージの一部として配布される。デモンストレーション版のプログラムは、ローダーセグメント、デモンストレーション版の解読キー、そしてデモンストレーション版の不正変更防止オーバーレイを含むように設計されている。この場合、不正変更防止オーバーレイには独自の使用許諾データは含まれないが、登録版の製品の箱と表示のデモンストレーションだけを付与するメインプログラムエグゼクティブ制御ルーブが含まれるであろう。デモンストレーション版のニグゼクティブ制御ルーブは、エグゼクティブ制御ルーブの総設計によって得られるプログラムの様々な特性を有している。たとえば、最終版を提供するデモンストレーション用ニューをプログラムして返戻版を表示することができるが、デモンストレーション版のエグゼクティブ

制御ルーブをプログラミングして返戻版を製品登録版として解釈して、製品を動作させる前に登録することを要求できる。

登録を開始する前に、見込み被読者はプログラムを実行し、デモンストレーション版が実行されよう。固定して図2に示したように、デモンストレーション版の解読キーが使用され、デモンストレーション版のエグゼクティブ制御ルーブがロード、解読、そして実行される。デモンストレーションが終了すると、見込み被読者は、使用者として登録し登録版のプログラムを被読するための一時的な使用許諾を得るようになる。そして、使用者は前述のようにして登録を行い、図2に示されているプロセスを開始することができる。登録要求に答えて、新しいオーバーレイファイル40'と独自の解読キー20'が含まれている製品ファイルが登録用コンピュータから送られる。追加プログラムファイルと更新版のプログラムファイルも、製品ファイルと共に受信される。登録プログラムはデモンストレーション版の不正変更防止オーバーレイ40と解読キー20をそれぞれの登録版40'と20'で置き替える。

登録に従い、使用者がプログラムを実行すると、プログラム実行過程で登録版の不正変更防止オーバーレイ40'が読み取られてロードされ、独自の解読キー20'を使用することにより、登録版のエグゼクティブ制御ルーブが解読され実行される。このようにして、デモンストレーション版は完全に動作する登録版に交換される。

プログラムの機能的な向上版が利用可能な場合、使用者は同一のプロセスを駆動してさらに別の解読キーと、より強化されたニグゼクティブ制御ルーブと追加プログラムファイルとを有する別の不正変更防止オーバーレイとを受信して、より強化された版の製品に更新することができる。

様々な実施例が、今をな不正変更防止オーバーレイを使用して大きなプログラムの解読を行なうための適切な施設を使

特表平6-501120 (7)

用することができる。このような技法は、ここにも含まれているように、プログラムの部分あるいはプログラム全体を使用許諾契約と結合する形式で配布するための、ここに開示されている方法がもたらす商業的利便の可能性の事なる例である。

上記の知見に照らし合わせ、本発明は種々の変形例が可能なのは明らかである。たとえば、本発明は、使用者のコンピュータがその地域の登録用コンピュータに接続され、さらにその登録用コンピュータがそれより広い地域の登録用コンピュータに接続され、というように階層構造的に実施することも可能である。その地域の登録用コンピュータの登録権限は、その地域の登録用コンピュータとそれより広い地域の登録用コンピュータとの間で含まれる使用許諾制御データによって制御できるであろう。したがって、下記の発明請求の範囲内であれば、本発明を上記明細書に説明されている以外の方法で実施することができる。

図 1

登録過程

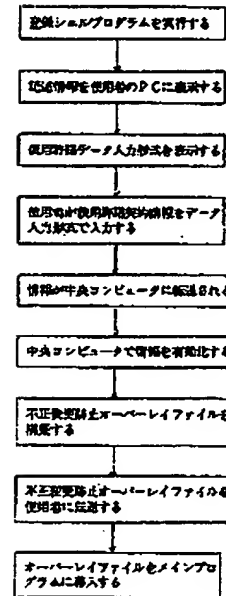
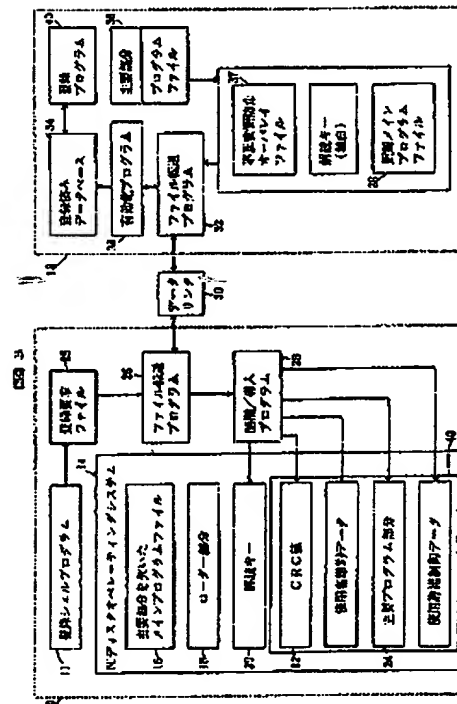
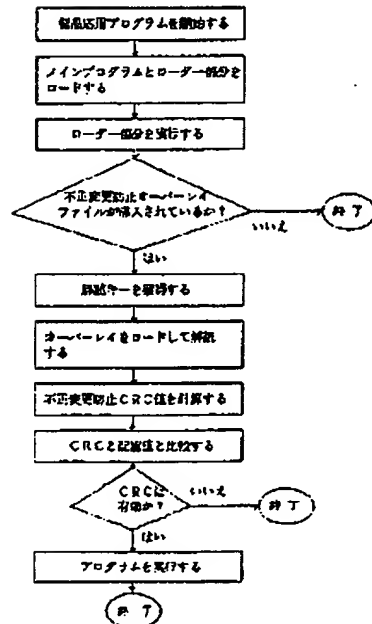
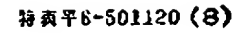


図 2

プログラム実行過程







國 庫 券 發 行

[illegible]

(S1) Int. Cl. 5

識別記号 斤内整理番号

F 1

H04L 9/12

(61) 指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IT, LU, NL, S E), CA, JP